AN NINH THÔNG TIN Ở VIỆT NAM TRONG ĐIỀU KIỆN HIỆN NAY - VẤN ĐỀ ĐẶT RA VÀ GIẢI PHÁP

❑ **Thiếu tướng, PGS. TS. LÊ VĂN THẮNG**
Giám đốc Học viện An ninh nhân dân

An ninh thông tin đã và đang đi vào mọi ngõ ngách của đời sống xã hội, dần trở thành một bộ phận quan trọng của an ninh quốc gia. Nhận diện rõ những vấn đề đang đặt ra, chủ động xây dựng những giải pháp bảo đảm an ninh thông tin là nhiệm vụ quan trọng, bức thiết để nâng cao hiệu quả bảo đảm an ninh thông tin của đất nước.

Trải qua 35 năm đổi mới, hệ thống thông tin của Việt Nam có sự phát triển mạnh mẽ, phục vụ đắc lực sự lãnh đạo, quản lý, điều hành của Đảng, Nhà nước, đáp ứng nhu cầu thông tin của xã hội, góp phần đảm bảo quốc phòng, an ninh của đất nước. Lĩnh vực viễn thông, Internet, tần số vô tuyến điện có sự phát triển mạnh mẽ, đạt được mục tiêu số hóa hoàn toàn mạng lưới, phát triển nhiều dịch vụ mới, phạm vi phục vụ được mở rộng, bước đầu hình thành những doanh nghiệp mạnh, có khả năng vươn tầm khu vực, quốc tế. Hệ thống bưu chính chuyển phát, báo chí, xuất bản phát triển nhanh cả về số lượng, chất lượng và kỹ thuật nghiệp vụ, có đóng góp quan trọng cho sự phát triển kinh tế - xã hội; đảm bảo quốc phòng, an ninh, đối ngoại của đất nước.

Tuy nhiên, tình hình an ninh thông tin ở Việt Nam đã và đang có những diễn biến phức tạp. Các thế lực thù địch, phản động không ngừng tăng cường hoạt động tình báo, gián điệp, khủng bố, phá hoại hệ thống thông tin; tán phát thông tin xấu, độc hại nhằm tác động vào chính trị nội bộ, can thiệp, hướng lái chính sách, pháp luật của Việt Nam; gia tăng các hoạt động tấn công mạng nhằm vào hệ thống thông tin quan trọng cũng như an ninh thông tin của nước ta.

Tội phạm và vi phạm pháp luật trong lĩnh vực thông tin diễn biến phức tạp, gia tăng về số vụ, thủ đoạn tinh vi, gây thiệt hại nghiêm trọng về nhiều mặt. Các hành vi phá hoại cơ sở hạ tầng thông tin; gây mất an toàn, hoạt động bình thường, vững mạnh của mạng máy tính, mạng viễn thông, phương tiện điện tử của các cơ quan, tổ chức, cá nhân và hệ thống thông tin vô tuyến điện,... đã và đang gây ra những thiệt hại lớn về kinh tế, xâm hại trực tiếp đến quyền, lợi ích hợp pháp của các cơ quan, tổ chức và cá nhân. Theo kết quả đánh giá an ninh mạng do Tập đoàn công nghệ BKAV thực hiện, trong năm 2019, chỉ tính riêng thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam đã lên tới 20.892 tỷ đồng (tương đương 902 triệu USD), hơn 1,8 triệu máy tính bị mất dữ liệu do sự lan tràn của các loại mã độc mã hóa dữ liệu tống tiền (ransomware), trong đó có nhiều máy chủ chứa dữ liệu của các cơ quan, gây đình trệ hoạt động của nhiều cơ quan, doanh nghiệp[2].

Thực tế trên đã làm xuất hiện nhiều nguy cơ đe dọa đến an ninh thông tin của Việt Nam ở cả bên trong và bên ngoài. Ở

Từ 2010 đến 2019, các cơ quan chức năng đã phát hiện trung bình mỗi năm trên 850.000 tài liệu chiến tranh tâm lý, phản động, ân xá quốc tế, tài liệu tuyên truyền tà đạo trái phép; gần 750.000 tài liệu tuyên truyền chống Đảng, Nhà nước được tán phát vào Việt Nam qua đường bưu chính. 53.744 lượt cổng thông tin, trang tin điện tử có tên miền ".vn" và".gov.vn" bị tấn công, trong đó có 2.393 lượt cổng thông tin, trang tin điện tử của các cơ quan Đảng, Nhà nước. Nhiều cuộc tấn công mang màu sắc chính trị, gây ra những hậu quả nghiêm trọng[1].

trong nước, trước hết là nguy cơ tụt hậu về công nghệ, lệ thuộc vào công nghệ của nước ngoài, nhất là hệ thống mạng lõi; phần mềm hệ thống, dịch vụ thông tin của nước ngoài (nhất là dịch vụ mạng xã hội) dẫn tới mất chủ quyền nội dung số, tài nguyên thông tin về các công ty công nghệ nước ngoài ngày càng nghiêm trọng hơn; các đối tượng cơ hội, chống đối chính trị thường xuyên sử dụng mạng xã hội tán phát thông tin giả, thông tin xấu, độc nhằm gây rối nội bộ, kích động biểu tình, bạo loạn.

Ở bên ngoài, các thế lực thù địch triệt để sử dụng hệ thống thông tin để tác động, can thiệp nội bộ, hướng lái chính sách, thao túng dư luận, thúc đẩy "cách mạng màu" ở Việt Nam; xâm phạm độc lập, chủ quyền quốc gia trên không gian mạng, tiến hành chiến tranh thông tin đối với Việt Nam. Các tổ chức phản động lưu vong, khủng bố tăng cường hoạt động tấn công, phá hoại hệ thống thông tin quan trọng về an ninh quốc gia; sử dụng không gian mạng để tán phát thông tin xấu, độc hại, kích động biểu tình, bạo loạn; hình thành các hội, nhóm, các tổ chức chính trị đối lập,... Các tổ chức tin tặc, tổ chức tội phạm thực

Từ 2001 đến 2019, các cơ quan chức năng đã phát hiện hơn 1.100 vụ lộ, mất bí mật nhà nước, trong đó lộ, mất bí mật nhà nước qua hệ thống thông tin chiếm tỷ lệ lớn với trên 80% số vụ[3].

hiện các cuộc tấn công mạng tự phát, đơn lẻ hoặc có chủ đích nhằm vào hệ thống thông tin trọng yếu quốc gia, làm tê liệt, gây gián đoạn hoạt động lãnh đạo, chỉ đạo, điều hành, quản lý kinh tế - xã hội của các cơ quan Đảng, Nhà nước.

Trong bối cảnh đó, các cơ quan, ban, ngành ở Trung ương và địa phương đã chú trọng nghiên cứu, xây dựng, áp dụng đồng bộ các giải pháp tăng cường đảm bảo an ninh thông tin. Bên cạnh những kết quả đã đạt được, công tác đảm bảo an ninh thông tin ở Việt Nam hiện nay đứng trước nhiều khó khăn, thách thức. Tiềm lực bảo đảm an ninh thông tin, cả về con người, tài chính và cơ sở hạ tầng kỹ thuật, công nghệ chưa đáp ứng yêu cầu đảm bảo an ninh thông tin trong tình hình mới; hiệu lực, hiệu quả quản lý nhà nước về an ninh thông tin chưa cao; năng lực phát hiện, xử lý các hoạt động xâm hại an ninh thông tin, sự cố gây mất an ninh thông tin của các cơ quan, đơn vị còn nhiều hạn chế; hiệu quả ứng dụng khoa học kỹ thuật trong đảm bảo an ninh thông tin chưa đáp ứng được yêu cầu, đòi hỏi của tình hình mới,...

Hiện nay, đất nước ta đang đứng trước những nguy cơ, thách thức lớn từ cuộc cách mạng công nghiệp lần thứ 4 với sự phát triển, ứng dụng mạnh mẽ của trí tuệ nhân tạo, rô-bốt, công nghệ sinh học, sẽ hình thành nên nhiều lĩnh vực mới như: "Internet công nghiệp", "Nhà máy thông minh", "Thành phố thông minh", "Xã hội siêu thông minh", "Chính phủ điện tử"... hoạt động trên môi trường không gian mạng, tạo sự đột phá về phát triển kinh tế, chính trị - xã hội. Xu hướng Internet kết nối vạn vật (IoT), gồm Internet kết nối với năng lượng, dịch vụ, truyền thông đa phương tiện, con người, vạn vật sẽ thay đổi phương thức hoạt động của cả một nền kinh tế, thói quen, tâm lý, văn hóa xã hội. Sự phát triển kinh tế - xã hội cũng như đảm bảo an ninh quốc gia ở Việt Nam những năm tới chủ yếu dựa trên nền tảng kỹ thuật số. Với xu thế phát triển của nền kinh tế chia sẻ, chuyển đổi số... công nghiệp công nghệ thông tin sẽ trở thành ngành kinh tế chủ đạo, quyết định sự phát triển nhanh, bền vững của quốc gia.

Thủ tướng Nguyễn Xuân Phúc dự lễ ra mắt Liên minh phát triển Hệ sinh thái sản phẩm an toàn, an ninh mạng Việt Nam.

An ninh thông tin là nội dung trọng tâm của an ninh quốc gia trong điều kiện mới, có mối quan hệ chặt chẽ với các vấn đề an ninh truyền thống khác như an ninh chính trị nội bộ, an ninh quân sự, an ninh văn hóa tư tưởng, an ninh kinh tế, an ninh xã hội.

Do đó, để nâng cao hiệu quả bảo đảm an ninh thông tin thời gian tới, cần quan tâm thực hiện đồng bộ các giải pháp sau:

Một là, nâng cao nhận thức về an ninh thông tin và bảo đảm an ninh thông tin. Cần nhận thức rõ, an ninh thông tin là độc lập, chủ quyền, lợi ích quốc gia trên không gian thông tin, sự an toàn, phát triển ổn định, vững mạnh của lĩnh vực thông tin, hệ thống thông tin quốc gia.

Nguy cơ gây mất an ninh thông tin là mối đe dọa lớn và ngày càng gia tăng đối với an ninh quốc gia, an ninh quốc tế. Chính vì vậy, đảm bảo an ninh thông tin là nhiệm vụ trọng yếu, thường xuyên của toàn Đảng, toàn dân, của cả hệ thống chính trị trong đó lực lượng Công an nhân dân là nòng cốt. Để đảm bảo an ninh thông tin cần coi trọng và sử dụng đồng bộ các biện pháp chính trị, pháp luật, khoa học kỹ thuật, tuyên truyền - giáo dục, tổ chức - hành chính, kinh tế, ngoại giao và nghiệp vụ chuyên môn.

Các cơ quan chức năng cần tăng cường giáo dục, bồi dưỡng, nâng cao ý thức của cán bộ, đảng viên và quần chúng nhân dân; chú trọng tuyên truyền, phổ biến cho học sinh, sinh viên về các nguy cơ, các yếu tố gây mất an ninh, đe dọa gây mất an ninh thông tin. Từ đó, nâng cao ý thức trong sử dụng các dịch vụ thông tin, nhất là dịch vụ do nước ngoài cung cấp; nâng cao bản lĩnh chính trị, khả năng nhận biết, tiếp nhận thông tin, khả năng tự vệ, "miễn dịch" trước những thông tin giả, thông tin xấu, độc hại. Có kế hoạch đưa nội dung về nhận diện các nguy cơ, yếu tố gây mất an ninh thông tin và trách nhiệm đảm bảo an ninh thông tin vào hệ thống giáo dục quốc dân, qua

đó giáo dục ý thức, trách nhiệm, nâng cao nhận thức cho toàn dân về vấn đề này.

Hai là, nghiên cứu xác lập chủ quyền quốc gia trên không gian mạng, bảo đảm giữ vững độc lập, tự chủ, chủ quyền và lợi ích quốc gia trên không gian thông tin quốc tế; bảo vệ và khai thác có hiệu quả tài nguyên thông tin quốc gia.

Việt Nam cần tiếp thu có chọn lọc kinh nghiệm quốc tế, tập trung nghiên cứu, xác lập không gian mạng quốc gia (với cơ sở hạ tầng, dịch vụ, khung pháp lý) nhằm sớm khẳng định chủ quốc gia trên không gian mạng. Xác định các yếu tố cấu thành và đẩy mạnh giải pháp nhằm thực thi có hiệu quả chủ quyền quốc gia trên không gian thông tin: 1) Phát triển công nghệ phần cứng nhằm bảo đảm tự chủ về phương tiện, thiết bị, nhất là hệ thống mạng lõi, máy tính, điện thoại, cơ sở hạ tầng thông tin; 2) Phát triển công nghệ phần mềm nhằm tạo lập hệ sinh thái phần mềm riêng, bao gồm hệ điều hành, công cụ tìm kiếm, mạng xã hội và các ứng dụng dịch vụ trên Internet; 3) Phát triển công nghệ bảo mật riêng và hệ thống kiểm tra, giám sát an ninh nhằm chủ động phát hiện và ngăn chặn, chặn lọc các thông tin giả, thông tin xấu, độc hại; 4) Xây dựng hệ cơ sở dữ liệu quốc gia tích hợp, liên thông, an toàn (Big Data) tạo thuận lợi cho quá trình chuyển đổi số và phát triển kinh tế số; 5) Xây dựng hệ thống tuyên truyền, định hướng thông tin hiện đại, an toàn và có trách nhiệm; hệ thống tấn công, phòng thủ riêng, đặc biệt là hệ thống thông tin trọng yếu của Đảng, Nhà nước và trên lĩnh vực an ninh, quốc phòng; 6) Xây dựng, hoàn thiện thể chế, chính sách, pháp luật và thị trường dịch vụ phát triển.

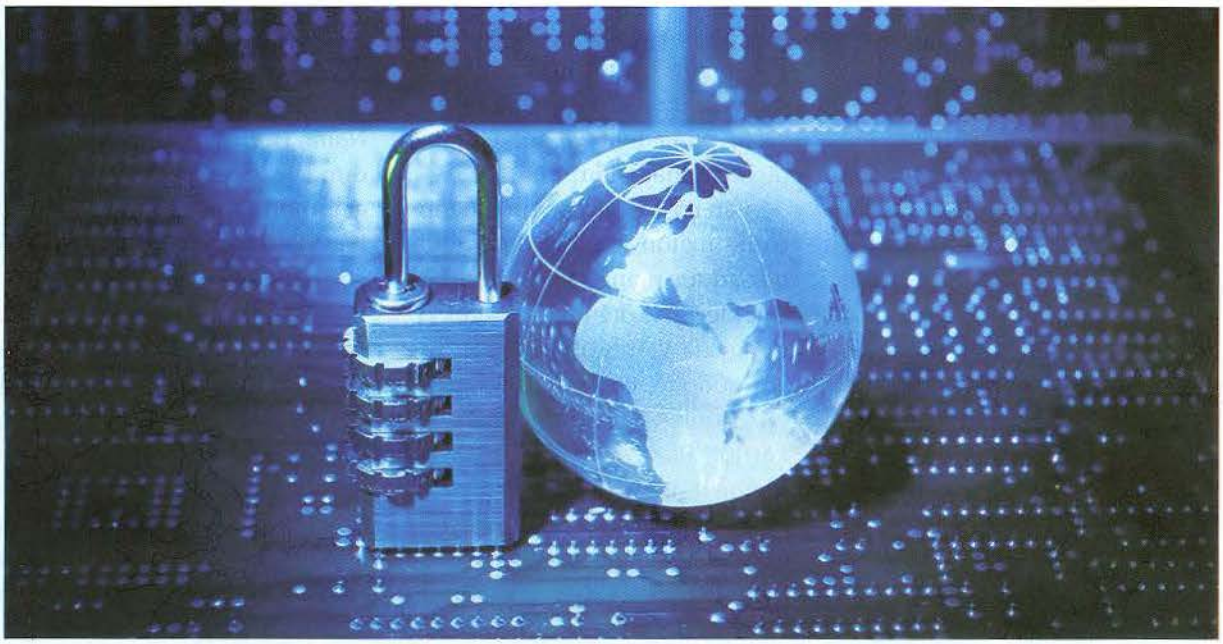
Cần có cơ chế đặc thù để tập trung nguồn lực xây dựng cho bằng được mạng xã hội, công cụ tìm kiếm, hệ điều hành tiện ích riêng của Việt Nam tương thích với quốc tế, có chỗ đứng vững chắc trên thị trường và trong xã hội. Điều này một mặt vừa khẳng định vị thế quốc gia, đảm bảo độc lập, tự chủ, chủ quyền quốc gia trên không gian mạng; từng bước hạn chế sự lệ thuộc vào công nghệ của nước ngoài; nâng cao khả năng bảo mật và khả năng tự chủ trong đảm bảo an ninh thông tin, đảm bảo lợi ích kinh tế quốc gia, tạo thuận lợi cho việc bảo tồn, phát huy giá trị văn hóa dân tộc, chủ động trong việc tiếp nhận thông tin và tạo thuận lợi trong thông tin, tuyên truyền của Đảng, Nhà nước; ngăn chặn có hiệu quả các thông tin xấu, độc hại, gia tăng khả năng đảm bảo bí mật thông tin cá nhân người dùng. Đồng thời cần có kế hoạch hợp lý khai thác và bảo vệ tài nguyên thông tin quốc gia phục vụ phát triển kinh tế, xã hội, đảm bảo quốc phòng an ninh.

Ba là, tăng cường sự lãnh đạo, chỉ đạo của Đảng, sự quản lý tập trung thống nhất của Nhà nước, nâng cao hiệu lực, hiệu quả quản lý nhà nước về an ninh thông tin.

Tập trung xây dựng, hoàn thiện chính sách, pháp luật về bảo đảm an ninh thông tin, tạo môi trường pháp lý để bảo đảm sự an toàn, tin cậy cho nền kinh tế số, cho việc chia sẻ dữ liệu số, cho quản lý hoạt động của các doanh nghiệp cung cấp dịch vụ thông tin qua biên giới vào Việt Nam. Tiếp tục nghiên cứu xây dựng luật về chống thông tin giả, thông tin xấu, độc hại; luật bảo vệ thông tin cá nhân. Có cơ chế công khai giám sát, chặn lọc thông tin xuyên tạc, sai sự thật trên không gian mạng; quy định cụ thể và thực hiện nghiêm túc quy định bắt buộc sử dụng thông tin thật khi đăng ký tài khoản trên mạng. Xây dựng bộ quy tắc ứng xử trên không gian mạng; quy định về bảo vệ, kiểm tra, sử dụng tài nguyên thông tin quốc gia, dữ liệu cá nhân người dùng.

Bốn là, bảo đảm tuyệt đối an toàn các hệ thống thông tin quan trọng quốc gia, hệ thống thông tin quan trọng về an ninh quốc gia, nâng cao năng lực phòng thủ, phục hồi sau các cuộc tấn công vào hệ thống thông tin, đấu tranh có hiệu quả với các hoạt động xâm phạm an ninh thông tin của các thế lực thù địch và các loại tội phạm.

Chính phủ cần tăng cường đầu tư cơ sở hạ tầng hiện đại, băng thông đủ rộng để vượt qua các cuộc tấn công gây nghẽn mạng, có hệ thống máy lưu trữ dự phòng để chuyển hướng dữ liệu trước các cuộc tấn công và phục hồi sau tấn công mạng. Thường xuyên rà soát, phát hiện, khắc phục lỗ hổng bảo mật trên toàn hệ thống, bổ sung thiết bị, phần mềm chuyên dụng có khả năng kiểm tra, kiểm soát an ninh, an toàn thông tin trên môi trường mạng viễn thông, Internet, tần số vô tuyến điện,... Xây dựng, triển khai thực hiện các giải pháp kỹ thuật chuyên



biệt nhằm kiểm tra, phát hiện các nguy cơ gây mất an ninh thông tin. Tổ chức diễn tập hàng năm về phòng, chống tấn công mạng cấp quốc gia với sự tham gia của cơ quan chính phủ, các tập đoàn kinh tế trọng yếu, các doanh nghiệp cung cấp dịch vụ viễn thông, Internet và các cơ quan, tổ chức có liên quan, đảm bảo xử lý kịp thời các nguy cơ gây mất an ninh, đe dọa gây mất an ninh thông tin ở Việt Nam.

Chú trọng dự báo, triển khai các giải pháp đấu tranh vô hiệu hóa hoạt động xâm hại an ninh thông tin của các đối tượng, nhất là hoạt động tấn công làm tê liệt hệ thống thông tin trọng yếu quốc gia; ý đồ sử dụng trí tuệ nhân tạo (AI), dữ liệu lớn (big Data) để thao túng, kích động dư luận xã hội, tạo điều kiện thúc đẩy "cách mạng màu" ở Việt Nam; và âm mưu, ý đồ của các thế lực thù địch, bá quyền quân sự hóa không gian thông tin, phát động chiến tranh thông tin đối với Việt Nam.

Năm là, tập trung nguồn lực để xây dựng, từng bước phát triển nền công nghiệp công nghệ thông tin, đặc biệt là công nghiệp an ninh thông tin (an ninh mạng) của Việt Nam.

Với nguồn lực của Việt Nam hiện nay, cần tập trung phát triển công nghiệp an ninh thông tin theo hướng lưỡng dụng, kết hợp cả trong lĩnh vực dân sự với bảo đảm an ninh, quốc phòng; đối tác công tư. Nhà nước cần có cơ chế đặc biệt, triển khai ngay các giải pháp đi tắt, đón đầu để từng bước làm chủ và xuất khẩu công nghệ thông tin. Khuyến khích nghiên cứu, phát triển, sử dụng các phần mềm, dịch vụ thông tin riêng của Việt Nam, đáp ứng yêu cầu bảo mật thông tin, sự an toàn của bí mật nhà nước, giám sát an ninh mạng. Xây dựng doanh nghiệp công nghệ thông tin, cung cấp dịch vụ viễn thông, Internet trong nước lớn mạnh, làm chủ thị trường, hình thành lực lượng doanh nghiệp cung cấp dịch vụ, có năng lực tự sản xuất các trang thiết bị an ninh thông tin.

Chính phủ cần ban hành cơ chế khuyến khích, hỗ trợ và huy động các tổ chức, cá nhân khởi nghiệp về công nghệ an ninh mạng, các doanh nghiệp công nghệ thông tin, cung cấp dịch vụ viễn thông, Internet trong nước làm chủ thị trường; hình thành các doanh nghiệp có năng lực tự sản xuất, cung cấp dịch vụ, các trang thiết bị, giải pháp gắn với bảo vệ an ninh mạng, tăng tỷ lệ nội địa hóa các sản phẩm công nghệ thông tin. Thành lập các quỹ đầu tư cho nghiên cứu, phát triển các giải pháp đảm bảo an ninh thông tin. ❑

---

(1) (3) Lê Văn Thắng (2019): *An ninh thông tin của Việt Nam trong điều kiện hiện nay: Thực trạng, vấn đề đặt ra và giải pháp*, Đề tài khoa học cấp Nhà nước.
(2) Tập đoàn BKAV (2019): *Báo cáo tổng kết công tác an ninh mạng năm 2019*.